THURSDAY, MARCH 25, 1897.

GALOISIAN ALGEBRA.[1]

Lehrbuch der Algebra. Von Heinrich Weber. Zweiter Band. Pp. xvi + 796. (Braunschweig: Vieweg und Sohn, 1896.)

IN one of Mrs. Barbauld's stories a domestic fairy, with one touch of her wand, transforms a tangled heap of parti-coloured silk into an orderly array of neatly wound skeins. Not unlike this is the effect of group-theory upon mathematical analysis; and it has been truly said that, for some time to come, the progress of analysis will be approximately estimated by the advance in our knowledge of the constitution of groups.

We have, therefore, good reason to be grateful to Prof. Weber for the very clear and masterly exposition of group-theory which is contained in the first three books of his second volume. It may be that we have read it at the psychological moment; in any case, it seems to us the clearest and most interesting account of the subject that we have seen.

In the spirit of Cayley's *dictum* that a group is defined by the laws of combination of its symbols, the author begins by a perfectly abstract definition of a group, and develops the theory of its normal and other divisors, the composition of its parts, and a series of important theorems on the decomposition of a group and its associated indices. The first chapter concludes with a further and more general discussion of metacyclic groups, already introduced in Vol. i.

Chapter ii., on Abelian groups, is substantially a revised and improved version of the author's well-known memoir in the *Acta Mathematica.* The discussion of the characters of an Abelian group, in particular, seems to us much more easy to understand than the corresponding part of the original memoir. The most important results in this chapter are the existence of a basis; the isomorphism of groups with the same invariants; the fact that to every divisor of an Abelian group, of index j, corresponds a set of exactly j characters, which for all elements of the divisor have the common value 1, while for every other element of the group at least one of the characters has a value different from unity; and, finally, that every divisor is associated with a definite reciprocal group whose degree is equal to the index of the divisor.

The next chapter, which again reproduces, in great measure, Prof. Weber's original memoir, contains a complete discussion of the groups of a cyclotomic corpus. It is impossible to give a brief analysis of this very important chapter: it must suffice to say that a definite algorithm is given for determining all cyclotomic corpora which correspond to a given set of invariants, and for constructing the associated cyclotomic periods. Chapter iv. contains applications of the general theory to cubic and biquadratic corpora, and a proof that all Abelian corpora of the third and fourth degrees are cyclotomic. In other words, the roots of an Abelian cubic or biquadratic equation with rational integral coefficients may always be expressed as rational and integral functions of roots of unity. This is a special case of a very remarkable theorem of Kronecker's, first proved by Prof. Weber, and demonstrated later on in the present work.

Chapter v. contains a further discussion of groups in general, and brings the reader fairly abreast of contemporary research. The very real advance which has been made in this subject in recent years may be said to date from the publication of Sylow's fundamental theorem that if n is the degree of a group and p^α a power of a prime which divides n, the group contains a divisor of degree p^α. A very simple inductive proof (after Frobenius) is given in this chapter; and this is followed by a series of propositions, hardly less important, and more or less depending upon it. Then we have a remarkable theorem, due to Frobenius, that if the degree of a group is not divisible by a square, it must be metacyclic; and the other one, also discovered by Frobenius, that every group whose degree is $p^\alpha q$, where p and q are different primes, is metacyclic. These theorems dispose of most groups whose degrees do not exceed 100: the rest are separately discussed in § 34, where references are given to the recent papers of Cole, Hölder, and Moore. It may be remarked that English mathematicians are devoting a good deal of attention to group-theory at present: reference might well have been made to the work of Askwith and Burnside. The last article of this chapter contains a proof of the theorem that the permutation-group of n letters contains no transitive and primitive divisor of index not exceeding n, except the alternate group of index 2; a further exception being made for $n=4$, and for $n=6$ respectively. Although the proof given is, of course, perfectly sound, it does not seem the truly ideal one; and it may very well happen that in this, as in other similar cases, a more appropriate demonstration will be ultimately discovered.

Book II. deals with linear groups, and in particular with the polyhedral and congruence groups with which the researches of Klein have made us so familiar. The polyhedral groups are exhibited in an analytical form, which makes it comparatively easy to discern their sub-groups; the proof that, besides the polyhedral groups, there are no other finite groups of the same type is after the manner of Gordon, and is remarkably simple in character. The decomposition of congruential groups (to a prime modulus) is effected very easily with the help of Galoisian imaginaries. The whole book may be profitably compared with the corresponding part of Klein's "Modulfunctionen," which, of course, traverses much the same ground.

Book III. contains various interesting applications of group-theory. The first chapter is on metacyclic equations, especially those of degree p^α, where p is a prime. It is shown that the Galoisian group of a primitive irreducible metacyclic equation of degree p^α is isomorphic with a linear congruence group (mod. p) of α variables; this group is compounded of a metacyclic group, isomorphous with

$$z'_i \equiv z_i + a_i \text{ (mod. } p),$$

and a *homogeneous* congruence group. Thus the problem of finding all such metacyclic equations is reduced to that of finding all the metacyclic divisors of the homogeneous congruence group. With the help of these results it is shown that all equations of the ninth degree with a linear congruence group are metacyclic, and a complete account is given of metacyclic equations of the degrees 4 and 8 respectively.

---

[1] The first volume of this work was reviewed in NATURE of November 12, 1896 (pp. 25–28).

The next two chapters illustrate the power of group-theory in dealing with a certain class of problems in analytical geometry. The configuration of the inflexional tangents of a plane cubic, and the much more complicated configuration of the twenty-eight double tangents of a quartic, are here reduced to the scheme of a group. The advantage thus gained is twofold: a clear comprehension of the structure of the configuration, and the appropriate engine for attacking the algebraic problems which the geometry suggests. Thus (p. 389) the fact that the Galoisian group of the equation of the twenty-eight double tangents of a quartic is simple and doubly transitive, is intimately connected with the existence of Steiner's sets of six associated pairs of double tangents; and the structure of the group shows the exact nature of the algebraical problem which consists in the separate determination of these sets of lines.

Chapter xiii. deals with the solution of the general quintic equation. It is now well known that the general quintic cannot be solved by radicals, and that it has no resolvent of lower degree than the sixth. By the solution of the quintic is now understood either the expression of its roots by means of transcendental functions, such as elliptic or modular functions; or else the expression of its roots in terms of a definite algebraical irrationality, such as that furnished by the icosahedral equation. The chapter before us is chiefly concerned with the second method; it is shown that the equation

$$y^5 + 5ay^2 + 5by + c = 0$$

where a, b, c are any constants whatever, may be identified with one of the principal resolvents (Hauptresolventen) of the icosahedral equation of the sixtieth degree, usually written in the form

$$T^2 - zf^5 = 0.$$

The process of identification requires the determination of z and of two other auxiliary parameters λ, μ, which fix the particular resolvent to be chosen. If Δ is the discriminant of the given quintic, the three auxiliary parameters are expressible as rational functions of a, b, c and $\sqrt{5\Delta}$. Ultimately, then, the roots depend in a quite simple way upon those of the icosahedral equation; this latter, although of a high degree, is very convenient of application, because its Galoisian group is known, and its roots are algebraical functions of a single parameter (z). Moreover, one of its roots may be simply expressed by means of the hypergeometric series (see p. 432). From this point of view then, if the solution of numerical quintics were a matter of practical importance, we should construct a single-entry table of the values of the icosahedral irrationality for different values of z, and then make use, in each particular case, of the formulæ of identification above referred to.

Chapters xiv. and xv. contain a theory of ternary groups of substitutions, and deal in particular with a group isomorphous with the G_{168}, which may be otherwise represented as a congruence-group, mod. 7. This admits of a very interesting application to a special class of equations of the seventh order, analogous to the use of the icosahedral equation in solving the quintic.

The fourth, and concluding, Book is on algebraical numbers; and to those whose predilections are arithmetical this will probably prove the most interesting of all. When Kummer generalised Gauss's theory of complex integers by introducing complex roots of unity of any order, he was at first baffled by the perplexing fact that in certain cases complex integers presented themselves which were incapable of resolution into factors, and yet did not possess all the essential qualities of prime factors; thus, for instance, one and the same number might be expressible both as $\alpha\beta$ and as $\gamma\delta$, where α and β were integers essentially distinct from γ and δ, and yet α, β, γ, δ were all indecomposible. By a stroke of unsurpassed genius, Kummer devised a theory of ideal primes, which at once removed the difficulty, and enlarged the province of arithmetic indefinitely. The divisibility of one real complex integer by another may be expressed by a series of linear congruences: Kummer succeeded in showing that, associated with every cyclotomic corpus, there are certain sets of congruential conditions which are precisely analogous in the general theory to divisibility by different primes in ordinary rational arithmetic. The satisfaction of one of these sets of congruences *may* denote divisibility by an actual (complex) prime; but whether this is so or not, the nature of the limitation thus imposed is just the same, and so, when the actual prime divisor does not exist, we say that the satisfaction of the congruential conditions expresses the existence of an *ideal* prime factor. As an example of how ordinary divisibility may be expressed by congruential conditions, we may take

$$ax + by \equiv 0,\ bx - ay \equiv 0 \pmod{a^2 + b^2}$$

which, if satisfied simultaneously, are equivalent to the divisibility of $x + yi$ by $a + bi$. Here, of course, when the congruences are satisfied, the complex factor $a + bi$ actually exists; but the congruences may be discussed, and their arithmetical significance developed, quite independently of this fact.

Kummer actually succeeded in showing how to construct, for any given cyclotomic corpus, the congruential conditions associated with the actual or ideal primes contained in it; but when his theory is extended to general algebraic corpora, it becomes impracticable to carry out the investigation precisely on Kummer's lines. The fundamental idea remains the same; and by an appropriate modification at the outset, Dedekind and Kronecker each succeeded in constructing an arithmetical theory capable of application to any corpus of algebraical integers whatever.

Their methods are not so different as at first sigh they may appear; this may be shown by an example which illustrates a fundamental point of the theory. Suppose that α and β are two ordinary rational integers; then the linear form $x\alpha + y\beta$, in which x, y assume all rational integral values, comprises a certain set of rational integers, and these are, in fact, the multiples of the greatest common measure of α and β. Thus, since a rational integer is given when all its multiples are given, we may say that the greatest common measure of α and β is represented by the linear form $x\alpha + y\beta$, or by the series of integers comprised in that form. Now this notion may be extended to the case when α and β are any two algebraical integers belonging to the same corpus; and the extension may be made in two ways. In Dedekind's theory x and y, as before, stand for rational integers, and our attention is directed not so much to the form $x\alpha + y\beta$ as to the series of numbers it represents. This series is called an ideal, and denoted by $[\alpha, \beta]$; so far as α and β are concerned, it is found to possess properties precisely analogous to those of the greatest common measure. Kronecker, on the other hand, keeps the form $x\alpha + y\beta$ explicitly, using x, y as mere symbols, or umbræ; and the highest common divisor of α and β is defined as follows. The norm of $x\alpha + y\beta$ is a rational homogeneous form in x, y which is the product of a rational integer and a primitive form F; by the highest common divisor of α and β we mean $(x\alpha + y\beta)/\mathrm{F}$. This definition has, of course, to be subsequently justified.

In a certain sense, then, the difference between the two methods is merely one of symbolic; but as in other similar cases (*e.g.* the methods of Cartesian and of homogeneous coordinates), it sometimes happens that propositions which are easily proved by the one are difficult for the other, and *vice versa*. Kronecker's theory was not worked out in detail in his famous "Festschrift"; Prof. Weber has now made it easily intelligible by adopting it, with some modification, as the basis of his exposition. Simplicity is gained by omitting primitive forms, such as F above, in the expression for divisors; and by means of a few new terms, such as "functional," the discussion is made at once concise and clear.

It should be added that the reader will find in this book not only a thorough account of the elements of the subject from Kronecker's point of view, but a guide to its most recent developments. Thus, for instance, it contains Minkowski's theorem on the minimum values of quadratic forms, with important applications to minimum representatives of ideal classes; and a summary of Hensel's very important investigations, by which it becomes possible to give an *explicit* representation of the prime ideals (or functionals) which belong to a given corpus.

Chapter xx., on quadratic corpora, shows the relation of Gauss's theory of quadratic forms to the general theory. Chapters xxi.-xxiv. are devoted mainly to the proof of Kronecker's theorem that all Abelian numerical corpora are cyclotomic; in other words, that the roots of *all* Abelian equations with rational integral coefficients are rational functions of roots of unity. The proof of this involves a long series of propositions, many of which are extremely valuable in themselves; we may instance the determination of the number of classes belonging to a given corpus, and the corollary that in every algebraical corpus there are an infinite number of prime ideals of the first degree. Perhaps the proof of Kronecker's theorem may some day be attained by a less laborious route; meanwhile it is a remarkable example of those arithmetical truths which are easily stated and easily understood, but, as yet, require for their demonstration an elaborate mathematical apparatus.

Prof. Weber's concluding chapter (xxv.), on transcendental numbers, contains a proof of the transcendence of e and π, and forms an elegant *coronis* for a work which is so important and so original that it is, to a great extent, above the range of ordinary criticism. As an introduction to, and exposition of, the theory of rational algebra and its arithmetical applications, it is simply invaluable. A student of real capacity, familiar with the technique of elementary algebra, may, by reading this work, together with Dedekind's wonderful tracts ("Ueber Stetigkeit," &c., and "Was sind u. was sollen die Zahlen?") and the last two editions of Dirichlet's "Zahlentheorie," equip himself for exploration in that strange unearthly region of arithmetic which attracts some sedentary spirits in much the same way as Arctic travel charms a Franklin or a Nansen. And even though he may not be one of the few who make discoveries of real importance, he will at least be able to appreciate intelligently the work that has been done, and the progress that has been made in developing the most abstract part of the only science that deserves to be called exact.

Gratitude has been defined by some practical cynic as the expectation of benefits to come: we must plead guilty to some such feeling on reading Prof. Weber's promise of a sequel, which is to deal with applications of the theory of algebraical numbers to the theory of elliptic functions; an application already partially carried out in his "Elliptische Functionen und algebraische Zahlen." And we cannot help remembering that, in conjunction with Prof. Dedekind, Prof. Weber has laid the foundations of a thoroughly arithmetical treatment of algebraic functions of one variable, in which alone (in our opinion) will be found a complete justification of the results to which Riemann was led by his geometrical method. Is it too much to hope that Prof. Weber may sometime be willing to develop these principles into a treatise on algebraical and Abelian functions? G. B. M.

THE WORSHIP OF TREES.

The Sacred Tree; or, the Tree in Religion and Myth. By Mrs. J. H. Philpot. Pp. xvi + 179. (London: Macmillan and Co., Ltd., 1897.)

THE further we are able to penetrate the mists which hang over the early history of mankind, the more sure we become that the primeval ancestors of our race regarded certain trees with veneration and awe; and it seems quite possible that in the earliest times the tree was a symbol of a supernatural and almighty power, which we might describe by the word "god." We shall not attempt to express in years the amount of the time which must have passed since tree worship began; but it will be sufficient, in the course of this short notice, to give a few proofs of its existence in the times which antedate the literature and history of all countries except those of Egypt and Southern Babylonia.

The study of the tree in its relation to religion and myth has occupied the minds of some of our best anthropologists, and though we are inclined to think that presently certain people will find the tree in every ancient piece of work and symbol—just as some investigators find the Christian cross everywhere, and others find the lotus in every ornament—still there is no